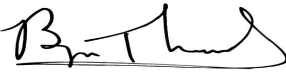


**RICHMOND POLICE DEPARTMENT GENERAL ORDER**

NOTE: This directive is for internal use only, and does not enlarge an employee's civil liability in any way. It should not be construed as the creation of a higher standard of safety or case in an evidentiary sense, with respect to third party claims. Violation of this directive, if proven, can only form the basis of a complaint by this Department, and then only in a non-judicial administrative setting.

Chapter 3	Number 4	Effective Date 11/02/09	Review Date 2012
Subject ACCESS TO COMPUTER APPLICATIONS			☐ New Order ☒ Replaces G.O. 3-4 (04/05/06)
References City of Richmond Administrative Regulations 2.3 (2/1/07), 2.11 (2/1/09)			
 _____ Chief of Police or Designee		11/02/09 _____ Date	

I. PURPOSE

The purpose of this Order is to establish the responsibilities and duties of Department employees concerning the proper use of the City's **Virtual Protocol Network (VPN)** and the procedures for requesting access to computer applications from the Records and Technology Division.

II. POLICY

It is the policy of the **City of Richmond and the** Richmond Police Department to manage access to computer applications to ensure that information remains secure and used only by authorized personnel in the performance of their duties. It also will provide access to its network for external users, such as consultants, special tasks force members and others, as deemed necessary, to conduct police department business. The Chief of Police or designee is responsible for ensuring that each user consistently complies with this policy. **VPN** access provides a means of connecting to the city's internal network via **a secure network tunnel**.

Annually, there will be an audit to verify security. A regular check of passwords and access codes will maintain the integrity of the system and security of the records contained in the system by the Records and Technology Division.

III. ACCOUNTABILITY STATEMENT

All employees are expected to fully comply with the guidelines and timelines set forth in this general order. Failure to comply will result in appropriate corrective action. Responsibility rests with the Division Commander to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated.

IV. PROCEDURE

A. Access to Computer Applications:

1. Employees shall submit all requests through their immediate supervisor who will approve and forward the request access to computer applications to the Records and Technology Division. The appropriate form to request access is the "Computer Application/Access Form" which is available on the server.
2. Upon receipt of the request, the Records and Technology Division will submit a formal request to the owner of the computer application who has the authority to grant or deny computer access to their files.
3. The owner's decision on whether access is granted or denied will be forwarded from the owner of the computer application to the Records and Technology Division who, in turn, shall notify the requester of the owner's decision.
4. The Records and Technology Division shall manage the requester's connection to the computer application(s) and shall notify the requester when access is available.

B. *Virtual Protocol Network (VPN)*:

1. Ownership:
 - a. All network systems, hardware, software, temporary or permanent files and any related systems or devices are the property of the City of Richmond. These include, but are not limited to, files, documents, spreadsheets, messages and notes that reside in part or in whole on any City of Richmond server, workstation, local area network (LAN) or individual computer.
 - b. Supervisors have the authority to inspect the contents of any hardware, software, document(s) or file(s) of their employees in the normal course of the supervisory responsibilities. The Police Computer Services Unit's staff and/or Department of Information Technology's staff shall extract information, files or documents when requested by authorized supervisory personnel. Reasons for review include but are not limited to:
 - 1) System, hardware and software problems;
 - 2) General system failure;
 - 3) A legal proceeding involving the City;
 - 4) Suspicion of a crime or violation of policy; or,
 - 5) A need to perform work or provide a service when the employee is unavailable.
2. Confidentiality/Privacy:

Employees using the city's data systems and/or tools provided by the City of Richmond have no guarantee of privacy with respect to the use of these systems and/or tools. Any files, documents, e-mails, electronic transactions or data of any kind that are created, stored or transported via the City's electronic data systems are considered the property of the City and are subject to inspection and review at any time. However, the foregoing notwithstanding, any and all opinions expressed while using these systems, whether implied or expressed, are those of the individual and not necessarily those of the City of Richmond or its management. Any messages, documents, spreadsheets or files are potentially a matter of public record and, thus, subject to disclosure.

3. Uses of *the VPN*:

- a. *The VPN*, hardware, software, tools and information are provided for the purpose of conducting business for the City of Richmond only.
- b. Allowable use of the network and information via *VPN* include the following, to the extent that these uses are for the purpose of conducting City of Richmond business:
 - 1) To facilitate performance of job functions;
 - 2) To conduct research in accordance with an employee's job duties and functions;
 - 3) To communicate with outside organizations as required in order to perform an employee's job functions; and,
 - 4) For personal communications/business, within reason, necessary as a result of employees performing their job functions.
- c. Prohibited uses of *VPN* and networked information includes, but are not limited to, the following:
 - 1) Illegal activities;
 - 2) Threats;
 - 3) Harassment;
 - 4) Slander;
 - 5) Defamation;
 - 6) Obscene or suggestive message(s) or obscene or offensive graphical image(s);
 - 7) Political endorsements; or,
 - 8) Commercial activities.

4. Installation and Servicing of *VPN*:

Unless otherwise specifically authorized by the Chief of Police or designee, **VPN** will be installed solely on computers owned by the Richmond Police Department. In the event that authorization for **VPN** services is granted for an employee's personally owned computer, the user agrees that operational problem identification and resolution by the Police Computer Services Unit will be limited solely to the proper functioning of the **VPN** components.

5. User Responsibilities:

The responsibilities of **VPN** users include:

- a. Any Department employee seeking **VPN** access shall request a **VPN** application from Police Computer Services to be signed and approved by the employee's OIC and forwarded to Police Computer Services.
- b. Maintaining the security of the employee's system and software through the appropriate use of a password known only to the user and generated via an encrypted security system.
- c. Users will receive information and instructions at the time the employee's **VPN** account is established.

6. Violations of Policy/Disciplinary Actions:

- a. Violations of this policy by Police Department employees can result in disciplinary action in accordance with the City of Richmond's Personnel Rules and other applicable Administrative Regulations, as well as any departmental rules, policies or regulations.
- b. Violations of this policy by non-City of Richmond employees granted special access to the City of Richmond network could result in the revocation of their access privileges and/or termination of their business relationship with the City of Richmond.

V. **ROLES AND ACCOUNTABILITY**

A. ***Employees requesting access to computer applications shall:***

1. ***Submit all requests through their immediate supervisor utilizing the "Computer Application/Access Form" which is available on the server; and,***
2. ***Use computer applications only for the purpose of conducting business for the City of Richmond.***

B. ***Employees requesting access to a VPN account shall:***

1. ***Complete and forward the VPN application to Police Computer Services;***
2. ***Maintain the security of the employee's system and software through the appropriate use of a password known only to the user and generated via an encrypted security system; and,***

3. *Use VPN only for the purpose of conducting business for the City of Richmond.*
- C. *Immediate supervisor of employees requesting access to computer applications shall:*
- Approve and forward requests for access to computer applications to the Records and Technology Division.*
- D. *Records and Technology Division personnel shall:*
1. *Audit passwords and access codes annually to maintain integrity of system and security of records;*
 2. *Submit a formal request to the owner of the computer application who has the authority to grant or deny computer access to their files, upon receipt of a request;*
 3. *Notify the requester of access to computer applications of the owner's decision;*
 4. *Manage the requester's connection to the computer application(s); and,*
 5. *Notify the requester when access is available.*
- E. *Police Computer Services Unit staff shall:*
1. *Extract information, files or documents when requested by authorized supervisory personnel; and,*
 2. *Only install VPN on computers owned by the Richmond Police Department, unless otherwise specifically authorized by the Chief of Police or designee.*
- F. *Supervisors shall:*
- Have the authority to inspect the contents of any hardware, software, document(s) or file(s) of their employees in the normal course of the supervisory responsibilities.*
- G. *Chief of Police or designee shall:*
1. *Be responsible for ensuring that each user consistently complies with this policy; and,*
 2. *Have the authority to authorize the use of VPN on computers.*

VI. FORMS

- A. *Computer Application/Access Form*
- B. *City of Richmond's Statement of Responsibility*